

CLAIMS

What is claimed is:

- 1 1. A service for managing a network boot of a client computer, the method comprising:
2 storing a list of trusted boot program servers in an interface service card coupled to a
3 client computer, the interface service card also being coupled to a hyper-secure remote service
4 network;
5 broadcasting a request for a boot program from the client computer to a network of boot
6 program servers;
7 receiving a response to the request for the boot program at the client computer, the
8 response being from a responding boot program server on the network of boot program servers;
9 comparing an identity of the responding boot program server with the list of trusted boot
10 program servers; and
11 upon verifying that the responding boot program server is on the list of trusted boot
12 program servers, requesting and downloading onto the client computer a boot program from the
13 responding boot program server.
- 1 2. The service of claim 1, further comprising:
2 upon determining that the responding boot program server is not on the list of trusted
3 boot program servers, blocking the requesting of the boot program from the responding boot
4 program server.
- 1 3. The service of claim 2, further comprising:
2 upon determining that the responding boot program server is not on the list of trusted
3 boot program servers, generating an alert to a designated administrator of a presence of an
4 unauthorized boot program server on the network of boot program servers.
- 1 4. The service of claim 1, wherein the designated administrator communicates with the
2 client computer via the hyper-secure remote service network.

1 5. The service of claim 4, wherein the comparing step is performed by configuring the blade
2 server to perform Layer 3 packet filtering to identify Pre-boot Execution Environment/Bootstrap
3 Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open
4 System Interconnection (OSI) model.

1 6. The service of claim 1, further comprising:
2 upon determining that the responding boot program server is not on the list of trusted
3 boot program servers, downloading a boot program from a known trusted boot server in a secure
4 local area network (LAN).

1 7. The service of claim 1, wherein the client computer is a server blade.

1 8. The service of claim 7, further comprising:
2 managing different types of boot program servers available to the server blade by
3 maintaining, in an information technology services organization logically oriented between the
4 different types of boot program servers and the server blade, a permission list of boot program
5 servers authorized for each server blade in a server blade chassis.